The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/01/2019

SUBJECT:
A Vulnerability in Exim Could Allow for Remote Command Execution

OVERVIEW:
A vulnerability has been discovered in Exim, which could allow for unauthenticated remote attackers to execute arbitrary system commands on the mail server. Exim is a mail transfer agent used to deploy mail servers on Unix-like systems. Successful exploitation of this vulnerability will enable the attacker to perform command execution as root in the context of the mail server. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
The vulnerability is relatively easy to exploit; it's probable that attackers will be searching for and exploiting vulnerable versions of this software soon. Proof of Concept code is available at https://bugs.exim.org/show_bug.cgi?id=2449 .

SYSTEMS AFFECTED:
Exim versions prior to 4.92.3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Exim, which could allow for unauthenticated remote attackers to execute arbitrary system commands by sending a large specially crafted Extended HELO (EHLO) string to the mail server.

This vulnerability exists due to a heap buffer overflow vulnerability within the string_vformat() function in string.c. This function does not account for the size of the input string and can

therefore lead to a buffer overflow condition. This can lead the mail server process to crash and potentially allow for remote code execution.

Successful exploitation of this vulnerability will enable the attacker to perform command execution as root in the context of the mail server. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Exim to vulnerable systems immediately after appropriate testing
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to open emails, download attachments, or follow links provided by unknown or untrusted sources.

REFERENCES:

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16928

Tenable:
https://www.tenable.com/blog/cve-2019-16928-critical-buffer-overflow-flaw-in-exim-is-remotely-exploitable

Exim:
https://www.exim.org/static/doc/security/CVE-2019-16928.txt
https://bugs.exim.org/show_bug.cgi?id=2449

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov